ABSTRACT

(Korean Patent Publication No. 2001-0047385)

The present invention relates to a method for generating a public key certificate in a certificate authority system in the case of issuance or renewal of the public key certificate for a user of a certificate authority.

The public key certificate generation method according to the present invention comprises an initialization step where an initial procedure is performed to issue the public key certificate, a step of managing a public key certificate request from the user, a step of executing a digital signature with respect to the public key certificate request and generating the public key certificate, a step of handing over a control to manage the generated public key certificate, and a step of managing login information according to each of the steps.

In response to the public key certificate request from the user, the present invention can perform a required work while maintaining the performance of the certificate authority system in its optimum state by executing a function for managing the public key certificate request. Further, the present invention can quickly provide the user with a result of the public key certificate request by

performing a function for managing the generated public key certificate.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.
H04L 9/14

(11) 공개번호 특2001-0047385
(43) 공개일자 2001년06월15일

(21) 출원번호 10-1999-0051586
(22) 출원일자 1999년11월19일

(71) 출원인 한국전자통신연구원, 오길록
대한민국
305-350
대전 유성구 가정동 161번지

(72) 발명자 임신영
대한민국
305-333
대전광역시유성구어은동한빛아파트107-303

하영국
대한민국
302-120
대전광역시서구둔산동향촌아파트115-302

강상승
대한민국
704-200
대구광역시달서구신당동1669-9

황호상
대한민국
305-333
대전광역시유성구어은동한빛아파트119동303호

박상봉
대한민국
137-060
서울특별시서초구방배동임광아파트2동306호

(74) 대리인 전영일

(77) 심사청구 없음

(54) 출원명 인증기관 시스템의 사용자용 공개키 인증서 생성 방법

요약

본 발명은 인증기관 사용자의 공개키 인증서 신규/갱신 발급에 대한 인증기관 시스템의 공개키 인증서 생성 방법에 관한 것이다.

본 발명의 공개키 인증서 생성 방법은 공개키 인증서 발급을 위한 초기화 과정, 사용자의 공개키 인증서 신청 요구를 관리하는 과정, 공개키 인증서 신청에 대하여 전자서명하여 공개키 인증서를 생성하는 과정, 생성된 공개키 인증서 관리를 위해 제어를 전환하는 과정 및 각 과정별 로그 정보를 관리하는 과정으로 이루어진다.

본 발명에 의하면 사용자의 공개키 인증서 신청에 대하여 사용자의 공개키 인증서 신청요구를 관리하는 기능을 통하여 인증기관 시스템의 성능을 최적의 상태로 유지하면서 요구 작업을 수행하게 되며, 생성된 공개키 인증서를 관리하는 기능을 통하여 사용자는 공개키 인증서 신청 결과에 대한 신속한 응답을 얻을 수 있다.

대표도

도1

명세서

도면의 간단한 설명

도 1은 본 발명에 의한 인증기관 시스템의 사용자용 공개키 인증서 생성 작업 정보 흐름도

도 2는 본 발명에 의한 인증기관 시스템의 공개키 인증서 생성을 위한 초기화 과정을 보인 흐름도

도 3은 본 발명에 의한 인증기관 시스템 사용자의 공개키 인증서 신청 요구를 관리하는 과정을 보인 흐름도

도 4는 본 발명에 의한 인증기관 시스템의 사용자용 공개키 인증서 생성 과정을 보인 흐름도

도 5는 본 발명에 의한 인증기관 시스템 내의 공개키 인증서 생성에서 공개키 인증서 생성 작업 기록 관리로 제어 전환하는 과정을 보인 흐름도

도 6은 인증기관의 사용자용 공개키 인증서 생성 작업 기록 관리 과정을 보인 흐름도

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 사용자의 공개키 인증서 신청에 대하여 인증기관 시스템의 성능을 최적의 상태로 유지하면서 신속하게 사용자용 공개키 인증서를 생성할 수 있는 인증기관 시스템의 사용자용 공개키 인증서 생성 방법에 관한 것이다.

공개키 암호 기술은 사용자가 각각 키쌍(Key Pair)을 생성하여 하나는 자신의 시스템 또는 시스템 외부에 보관하는 개인키(Private Key)로 사용하고 다른 하나는 공개하는 공개키(Public Key)로 하여 제 3 자가 이 공개키를 이용하여 수신자에게 평문을 암호문으로 만들어 보내면 수신자 즉, 공개키 소유자는 자신의 공개키에 해당하는 개인키를 암호문에 수학적으로 대입함으로써 암호문을 평문으로 만들어 그 내용을 수신자가 볼 수 있도록 하는 것이 공개키 암호 기술의 핵심이다.

공개키 암호 기술을 사용하기 위하여 즉, 공개키를 안전하게 공개하기 위하여 사용자는 신뢰할 만한 기관 즉, 인증기관에 자신의 공개키를 등록하는 것이 필요하다.

이는 자신의 공개키에 대한 전자서명을 인증기관에 요구하여 인증기관의 전자서명이 첨부된 공개키 인증서를 발급받아, 이를 다른 인증기관 가입자들이 용이하게 획득할 수 있도록 하여 공개키 암호 기술을 사용할 수 있는 기반을 제공하는 것을 의미한다.

이러한 공개키 인증서를 인증기관 시스템이 발급하는 과정에서 사용자의 신청 건수와 시스템의 처리 용량의 균형있는 시스템 관리를 통하여 인증기관 시스템의 최적화와 사용자 서비스 관리를 보장할 수 있다. 이를 위하여 인증기관 시스템은 사용자의 공개키 인증서 신청 요구에 대하여 효과적으로 서비스를 제공할 수 있도록 인증기관 시스템 관리의 기술적 방법이 요구된다.

그런데, 종래에는 이러한 공개키 인증서를 발급함에 있어 인증기관 시스템은 공개키 인증서 신청 요구 관리, 공개키 인증서 생성, 생성된 공개키 인증서 관리 및 인증기관 시스템에서 수행한 작업 기록 정보 관리를 모두 하나의 모듈 내에서 처리하였다. 때문에 인증기관 시스템이 운용이 효율적이지 못할 뿐아니라 사용자에게도 효과적인 서비스를 제공할 수 없었다.

발명이 이루고자 하는 기술적 과제

본 발명은 상기한 종래의 문제점을 해결하기 위하여 안출된 것으로서, 사용자의 신분 확인이 완료된 사용자 공개키 인증서 신청 접수에 의해 인증기관 시스템의 성능을 최적의 상태로 유지하면서 신속하게 사용자용 공개키 인증서를 생성할 수 있는 방법을 제공하는 데 그 목적이 있다.

발명의 구성 및 작용

상술한 목적을 달성하기 위하여, 본 발명은 인증기관 시스템이 최초로 시동되는 시점에 공개키 인증서 발급 기능의 초기화 과정을 수행하는 방법, 사용자들이 신청한 공개키 인증서 신청 작업 건에 대한 요구를 관리하는 방법, 사용자의 공개키 인증서 신청에 대하여 인증기관의 서명용 개인키로 전자서명하여 그 결과값, 전자서명값을 사용자의 공개키 인증서 신청 정보에 첨부함으로써 공개키 인증서를 생성하는 전자서명 방법, 사용자의 공개키 인증서 신청에 대한 공개키 인증서 생성이 완료된 후 공개키 인증서 관리를 위한 제어전환 방법, 및 인증기관 시스템에서 수행한 작업 기록 정보(예 : 초기화 작업, 사용자 요구 접수, 사용자 공개키 인증서 생성, 제어 변경, 종료)를 보관하고 있는 로그 정보 관리 방법을 제공하며, 이들은 각각 별개의 모듈로 구성되는 것을 특징으로 한다.

본 발명의 설명에 앞서, 본 발명에서 사용하고 있는 용어에 대한 정의는 다음과 같다.

개인키(Private Key)

공개키(비대칭키) 암호 기술을 사용하기 위하여 사용자 또는 인증기관에서 생성하는 키쌍으로 공개키(Public Key)와 개인키(Private Key)가 있다. 이 중 공개키는 인증기관에 등록하여 공개키를 다른 사람이 이용하여 메시지 송수신 암호 기술에 사용하도록 공개하며, 개인키는 개인이 안전한 곳(통상 스마트 카드)에 보관한다.

세션키(Session Key, Secret Key)

전자문서 원문을 암호화하는데 사용하는 키로 비밀키(대칭키) 암호 기술이 적용된다. 세션키는 비밀키로 부를 수 있으며 세션키는 사용자 측에서 난수를 생성하여 일회용으로 사용한다.

CA(Certification Authority)

인증기관으로서 사용자 및 시스템 관리자를 위한 공개키 인증서를 생성하여 관리하는 시스템이다. 초기화 시 사용자용 공개키 인증서 확장정보에 인증기관 가입자 관련 고유 정보(특정 기업명, 서비스명 등)를 기재하기 위한 인증기관 정보의 정의를 수행한다.

이하, 본 발명의 바람직한 실시예를 첨부도면을 참조하여 상세하게 설명한다.

도 1은 본 발명에 의한 인증기관 시스템의 사용자용 공개키 인증서 생성을 위한 정보 흐름도이다.

도면에서, 사용자의 공개키 인증서 신청 요구가 인증기관 시스템에 수신된 이후부터 사용자의 공개키 인증서 생성이 완료되어 인증기관 시스템 내부의 공개키 인증서 관리 모듈로 제어가 변경되는 시점까지의 정보 흐름을 총체적으로 나타낸 것이다.

이를 설명하면, 인증기관 시스템이 후술하는 공개키 인증서 생성을 위한 초기화 과정을 마친 상태에서 사용자의 공개키 인증서 신청(1)이 인증기관 시스템에 수신되면, 인증기관 시스템은 이를 선입선출 방식의 공개키 인증서 신청 대기열(2)에 저장한다.

다음에, 상기 신청 대기열(2)에 저장된 공개키 인증서 신청에 대한 요구들은 그 신청된 순서대로 공개키 인증서 생성 모듈(3)에서 전자서명되어 공개키 인증서가 생성된다.

그리고, 인증기관 시스템은 신청 대기열(2)의 하나의 공개키 인증서 신청에 대해 공개키 인증서 생성이 완료되면, 공개키 인증서 관리모듈(4)로 제어를 전환하여 공개키 인증서 생성에 관련된 작업 기록을 관리한다.

또한 공개키 인증서 생성 작업 로그 관리모듈(5)에 의해 공개키 인증서 신청 요구 관리와 전자서명 작업 수행 후 그 내역이 관리된다

이하, 사용자용 공개키 인증서 생성을 위한 과정을 도 2 내지 도 6을 참조하여 설명한다.

도 2는 본 발명에 의한 인증기관 시스템의 공개키 인증서 생성을 위한 초기화 과정을 보인 흐름도이다.

먼저, 인증기관 시스템이 인증기관 관리자의 구동명령 입력(관리자 암호, 구동 명령어 입력)에 의해 인증기관 관련 프로그램을 구동시킨다(S201, S202).

다음에, 인증기관의 서명용 및 암호용 키쌍을 보유하고 있는지를 확인하여(S203), 보유하고 있으면 키쌍을 임시 저장소에 보관한 다음(S204), 단계 S206을 수행한다.

단계 S203에서 확인결과 인증기관의 서명용 및 암호용 키쌍을 보유하고 있지 않는 경우(최초 구동)와 단계 S204를 수행한 후에, 인증기관 시스템의 암호용 및 서명용 키 쌍을 생성한 다음, 생성된 암호용 및 서명용 키 쌍 중 공개키 2개를 상위의 인증기관에 오프라인 방식으로 등록하기 위하여 인증기관 담당자는 상위 인증기관 담당자를 방문하여 2개의 공개키에 대하여 공개키 인증서를 발급 받는다(S205).

인증기관 시스템의 사용자 공개키 인증서 생성 모듈이 정상 구동 여부의 확인은 관리자가 인증기관 관리자 메뉴를 초기화하면서 관리자 계정 및 암호 그리고 상위 인증기관에서 발급 받은 공개키 인증서에 해당하는 암호용 개인키를 제시한 다음, 관리자 메뉴를 선택하여 메뉴상의 공개키 인증서 생성 현황을 선택할 경우, 메뉴 제목과 현황 정보를 알려주는 빈 내용의 테이블이 화면에 나타나면 정상적으로 공개키 인증서 생성 모듈이 동작한다고 판단할 수 있다.

도 3은 본 발명의 공개키 인증서 신청 요구 관리 모듈에 의한 인증기관 시스템의 공개키 인증서 신청 요구를 관리하는 과정을 보인 흐름도이다.

사용자는 인증기관으로부터 온라인으로 공개키 인증서를 발급받기 위한 사전작업으로 인증기관에서 사용자용 소프트웨어를 인터넷을 통하여 다운로드받아 사용자 시스템에 설치한다.

이 상태에서 사용자는 사용자 시스템에 설치된 인증기관 사용자용 소프트웨어를 구동하여 메뉴상의 사용자 공개키 인증서 신청(또는 사용자 공개키 인증서 갱신)을 선택하여 해당 정보를 입력하여 신규/갱신 신청 양식을 작성한다(S301).

공개키 인증서 신청 정보에는 신청자 성명, 전자우편 주소, 우편주소, 직장명, 소속부서, 전화번호, 공개키 인증서 취소리스트 배포(실시간, 기본), 용도등이 있다.

신규/갱신 공개키 인증서 신청양식의 사용자 입력 내용을 점검하여 오류 및 예외 정보가 없을 때까지 단계 S301 내지 단계 S303을 반복 수행한다.

작성된 신규/갱신 공개키 인증서 신청양식의 입력 내용에 오류 및 예외 정보가 없으면 사용자 소프트웨어 내부에서는 사용자를 위한 2종류의 사용자 키 쌍 즉, 암호용 및 서명용 키 쌍을 생성하고, 이 중 공개키 2개를 사용자의 공개키 인증서 신청(또는 갱신) 메시지에 첨부하여 인증기관에 송신한다(S304).

이를 상세하게 설명하면, 사용자 시스템과 인증기관 시스템간에는 공개키 암호 기술을 이용한 송수신 메시지의 암호 처리를 수행한다.

메시지 암호 처리를 수행하는 방법은 송신할 메시지를 세션키로 대칭키 암호화를 수행하여 메시지 암호문을 생성한다(A). 그리고 송신하는 메시지 원문에 대하여 해쉬 함수 처리하여 사용자의 서명용 개인키로 서명한 서명값(B)을 송신하는 정보에 추가한다. 사용자 시스템의 인증기관 사용자용 소프트웨어내에 내장된 인증기관의 암호용 공개키를 사용하여 세션키에 대하여 공개키 암호화를 수행하여 전자봉투를 생성한다(C).

사용자는 송신 메시지 원문에 대하여 대칭키 암호화한 암호문, 전자봉투 및 서명값을 인증기관에 송신한다.

이와 같이 사용자가 공개키 인증서 신청 양식을 작성하여 인증기관 시스템에 전송하면, 인증기관 시스템은 사용자가 송신한 공개키 인증서 신청 정보에 대하여 인증기관의 암호용 개인키로 전자봉투를 열어 세션키를 획득하고(S305), 이 세션키를 암호문에 대입하여 메시지 원문을 획득한다(S306).

다음, 전자서명한 서명값을 이용하여 메시지 원문의 무결성을 확인한다. 이 작업은 사용자 시스템과 인증기관 시스템간의 메시지 송수신의 모든 경우에 해당된다.

메시지 원문의 무결성 확인은 해독한 메시지 원문에 대해 해쉬 함수를 수행하여 해쉬값(D)을 획득하고(S307), 이를 사용자 시스템에서 수신한 전자서명값(B)에 대해 역해쉬 함수를 수행하여 얻은 해쉬값(B')과 비교함으로써 이루어진다(S308, S309).

메시지 원문에 결함이 있으면(B'≠D) 사용자 시스템에 오류 메시지를 전송(S311)하고, 메시지 원문의 무결성이 확인되면(B'=D) 인증기관은 사용자가 송신한 공개키 인증서 신청 요구를 인증기관 시스템 내부에 설정한 공개키 인증서 신청 요구 대기열에 위치시킨 뒤 대기열 번호를 내림차순으로 부여한다(S310).

이후, 인증기관 시스템은 부여한 대기열 번호의 내림차순으로 공개키 인증서 신청 요구 대기열의 사용자의 공개키 인증서 신청 요구 사항을 수행한다.

도 4는 본 발명의 공개키 인증서 생성 모듈에 의한 인증기관 시스템의 사용자용 공개키 인증서 생성 과정을 보인 흐름도로서, 인증기관의 공개키 인증서 신청 요구 대기열에 저장되어 있는 사용자의 공개키 인증서 신청 요구를 내림차순으로 처리하여 사용자용 공개키 인증서를 생성한다.

상세하게 설명하면, 먼저 인증기관은 시스템 내부에 접수된 사용자의 공개키 인증서 신청 요구 대기열의 번호 순번(내림차순)에 따라 대기열에서 사용자 신청 요구 정보를 시스템 메모리로 읽은 후, 인증기관 시스템내에서 독립된 형태의 프로그램으로 전자서명 작업을 별도로 수행하도록 전자서명 부프로그램을 시스템 내부에서 구동한다(S410, S420).

전자서명 부프로그램(S430)은 인증기관 시스템 내부로 읽은 사용자 신청 요구 정보에 대하여 다음과 같이 전자서명을 수행하여 공개키 인증서를 생성한다.

먼저, 전자서명 부프로그램은 사용자 공개키 인증서 신청 메시지를 저장한 다음(S431), 사용자 신청 요구 정보를 공개키 인증서 양식에 대한 정보 구조로 변경한다(S432). 그런 다음, 변경된 정보 구조에 대하여 인증기관의 서명용 개인키로 서명한 서명값을 공개키 인증서 정보 구조 말단에 첨부함으로써 사용자의 공개키 인증서를 생성한다(S433).

도 5는 본 발명에 의한 인증기관 시스템 내의 공개키 인증서 생성에서 공개키 인증서 관리로 제어 전환하는 과정을 보인 흐름도이다.

도 4에서와 같이 생성된 사용자의 공개키 인증서는 공개키 인증서 생성 모듈과 병렬로 동작되는 인증기관 시스템 내부의 공개키 인증서 관리 모듈로 전송되어 사용자에게 전송하는 등의 후속 작업을 수행하도록 한다.

상세하게는, 하나의 공개키 인증서 신청 요구에 대해 공개키 인증서 생성을 완료하면 인증기관 시스템은 전자서명 부프로그램 종료 명령으로 공개키 인증서 생성 모듈의 작업을 종료하면서, 사용자 공개키 인증서 신청 접수시점부터 공개키 인증서 생성 모듈 작업 종료 시점까지 수행한 작업 로그와 생성한 공개키 인증서를 출력한다(S501)

다음에, 상기 공개키 인증서 생성 모듈 작업 종료의 출력물인 작업 로그와 공개키 인증서를 공개키 인증서 관리 모듈로 전송함으로써 공개키 인증서 생성 모듈에서 공개키 인증서 관리 모듈로 제어를 변경되고(S502), 사용자 공개키 인증서 신청 작업 결과물은 공개키 인증서 관리 모듈에서 처리된다

그리고, 공개키 인증서 관리 모듈로부터 수신 결과의 정상 처리를 통보 받으면 공개키 인증서 생성 모듈의 대기열을 점검하여 대기열에 남은 사용자 요구를 순차 처리한다(S503).

도 6은 본 발명의 공개키 인증서 생성 작업 로그 관리 모듈에 의한 인증기관의 사용자용 공개키 인증서 생성 작업 기록 관리 과정을 보인 흐름도로서, 공개키 인증서 신청 요구 관리, 공개키 인증서 생성 및 공개키 인증서 관리와는 병렬로 처리된다.

공개키 인증서 생성 작업 기록 정보는 다음의 세부 정보 사항을 정의하여 기록, 유지 및 조회할 수 있도록 한다.

1. 인증기관 시스템의 초기화 관련 정보로서, 초기화 시 공개키 인증서 생성 모듈의 초기 구동 일시 및 구동된 프로그램 이름(공개키 인증서 생성 모듈, 공개키 인증서 신청 대기열 관리 모듈, 공개키 인증서 대기열 이름/대기열 처리 용량(통상 50개의 대기열로 정의되며 시스템의 환경에 따라 조정 가능함), 전자서명 부프로그램 관리 모듈(공개키 인증서 생성 마스터 프로그램) 및 전자서명 부프로그램 모듈(공개키 인증서 생성 슬레이브 프로그램))

2. 사용자 요구 관리 정보로서, 인증기관의 사용자 공개키 인증서 신청/갱신 요구 수신 일시, 송신처 정보(송신 시스템의 호스트 주소, 송신자 성명), 인증기관의 대기열 대기번호 발급 건수, 대기열에서 대기한 요구 건수, 대기열에서 처리된 요구 건수

3. 전자서명 작업 정보로서, 전자서명 부프로그램 별 수행 일시, 수행 소요 시간(초) 및 수행 결과(성공, 인증기관 프로그램 장애로 인한 실패, 시스템 장애로 인한 실패) 및 일자별 전자서명 부프로그램 총 수행건수

4. 종료 관련 정보로서, 인증기관 시스템 종료 시 공개키 인증서 생성 모듈 종료 일시 및 프로그램 종료 결과(정상 종료, 비정상 종료)

인증기관 관리 정책에 따라 공개키 인증서 생성 작업 기록의 안전한 관리를 위하여 일정 주기마다 상기한 공개키 인증서 생성 작업 기록 정보 전체에 대하여 전자서명 시점의 기록정보 사본(A)를 생성하고, 이를 인증기관의 서명용 개인키로 서명하여 전자서명값(B)를 획득한다(S601~S603).

서명값은 인증기관 관리자가 인증기관 시스템 내부 및 외부에 저장한다.

서명값을 시스템 내부에 저장할 경우, 기록정보를 인증기관 관리자 암호로 암호 처리하여 암호된 기록정보 사본과 전자서명값을 획득하고(S604), 또 이에 전자서명 수행 시각 정보(D)를 포함시켜 공개키 인증서 생성 작업 정보 테이블로서 관리한다(S605).

한편, 서명값을 시스템 외부에 저장할 경우에도 시스템 내부에 저장하는 경우와 동일하게 관리자가 작업하되 외부의 저장 매체 저장한다.

발명의 효과

상술한 바와 같이 본 발명은 사용자의 공개키 인증서 신청에 대하여 인증기관 시스템이 성능을 최적의 상태로 유지하면서 공개키 인증서를 생성할 수 있는 효과가 있으며, 이로 인해 사용자는 공개키 인증서 신청 결과에 대한 신속한 응답을 얻을 수 있다.

이상에서 본 발명에 대한 기술사상을 첨부도면과 함께 서술하였지만 이는 본 발명의 바람직한 실시예를 예시적으로 설명한 것이지 본 발명을 한정하는 것은 아니다. 또한, 이 기술분야의 통상의 지식을 가진 자라면 누구나 본 발명의 기술사상의 범주를 이탈하지 않는 범위 내에서 다양한 변형 및 모방이 가능함은 명백한 사실이다.

(57) 청구의 범위

청구항 1.
인증기관 시스템의 사용자용 공개키 인증서 생성 방법에 있어서,

인증기관 시스템이 최초로 시동되는 시점에 공개키 인증서 발급 기능의 초기화 과정을 수행한 상태에서, 사용자들이 신청한 공개키 인증서 신청 요구를 수신하여 관리하는 공개키 인증서 신청 요구 관리 과정과;

공개키 인증서 신청 요구 대기열의 공개키 인증서 신청 요구에 대하여 인증기관의 서명용 개인키로 전자서명하여 그 결과값, 전자서명값을 사용자의 공개키 인증서 신청 정보에 첨부함으로써 공개키 인증서를 생성하는 과정과;

사용자의 공개키 인증서 신청에 대한 공개키 인증서 생성이 완료된 후 공개키 인증서 관리를 위하여 제어를 전환하는 과정; 및

인증기관 시스템에서 수행한 작업 기록 정보(예: 초기화 작업, 사용자 요구 접수, 사용자 공개키 인증서 생성, 제어 변경, 종료 등)를 보관하고 있는 로그 정보를 관리하는 과정을 포함하며, 상기 과정들이 개별 모듈로 구성되는 것을 특징으로 하는 인증기관 시스템의 사용자용 공개키 인증서 생성 방법.

청구항 2.
제1항에 있어서,

상기 공개키 인증서 신청 요구 관리 과정은

사용자가 송신한 공개키 인증서 신청 정보에 대하여 인증기관의 암호용 개인키로 전자봉투를 열어 세션키를 획득하고, 이 세션키를 암호문에 대입하여 메시지 원문을 획득하는 단계와;

해독한 메시지 원문에 대해 해쉬 함수를 수행하여 해쉬값(D)을 획득하고, 이를 사용자 시스템에서 수신한 전자서명값(B)에 대해 역해쉬 함수를 수행하여 얻은 해쉬값(B')과 비교하여 무결성을 확인하는 단계; 및

메시지 원문에 결함이 있으면(B'≠D) 사용자 시스템에 오류 메시지를 전송하고, 메시지 원문의 무결성이 확인되면(B'=D) 사용자의 공개키 인증서 신청 요구를 인증기관 시스템 내부에 설정한 공개키 인증서 신청 요구 대기열에 위치시킨 뒤 대기열 번호를 내림차순으로 부여하는 단계를 포함하는 것을 특징으로 하는 인증기관 시스템의 사용자용 공개키 인증서 생성 방법.

청구항 3.
인증기관 시스템에서 사용자용 공개키 인증서를 생성하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체에 있어서,

인증기관 시스템이 최초로 시동되는 시 점에 공개키 인증서 발급 기능의 초기화 과정을 수행한 상태에서, 사용자들이 신청한 공개키 인증서 신청 요구를 수신하여 원문의 무결성이 확인되면 사용자가 송신한 공개키 인증서 신청 요구를 공개키 인증서 신청 요구 대기열에 위치시킨 뒤 대기열 번호를 부여하여 관리하는 공개키 인증서 신청 요구 관리 과정과;

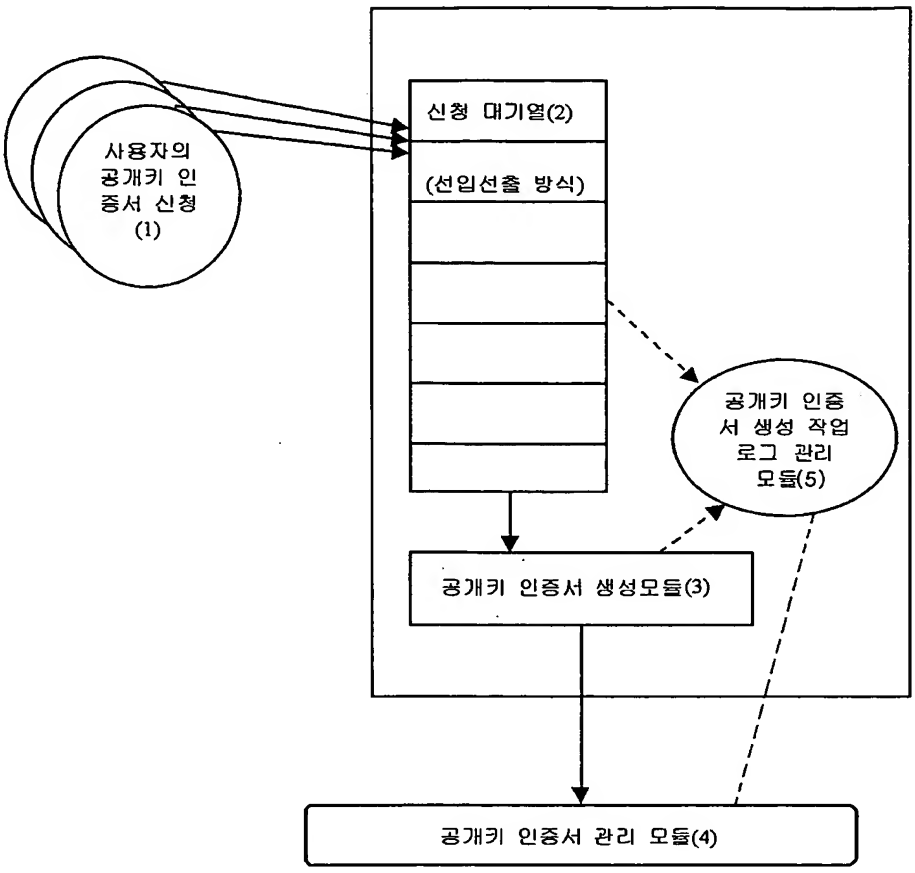
공개키 인증서 신청 요구 대기열의 공개키 인증서 신청 요구에 대하여 인증기관의 서명용 개인키로 전자서명하여 그 결과값, 전자서명값을 사용자의 공개키 인증서 신청 정보에 첨부함으로써 공개키 인증서를 생성하는 과정과;

사용자의 공개키 인증서 신청에 대한 공개키 인증서 생성이 완료된 후 공개키 인증서 관리를 위하여 제어를 전환하는 과정; 및

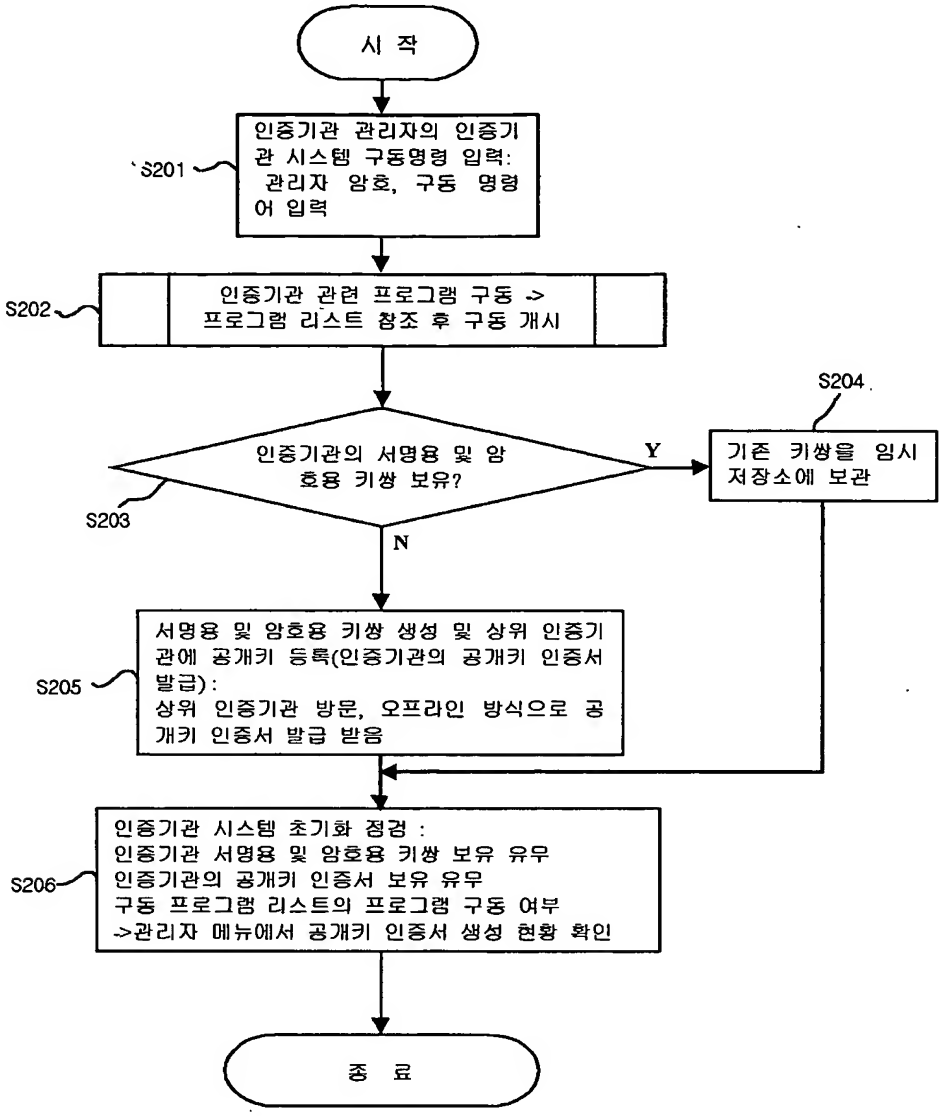
인증기관 시스템에서 수행한 작업 기록 정보(예: 초기화 작업, 사용자 요구 접수, 사용자 공개키 인증서 생성, 제어 변경, 종료 등)를 보관하고 있는 로그 정보를 관리하는 과정을 포함하며, 상기 과정들이 개별 모듈로 구성되는 실행시킬 수 있는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체.

도면

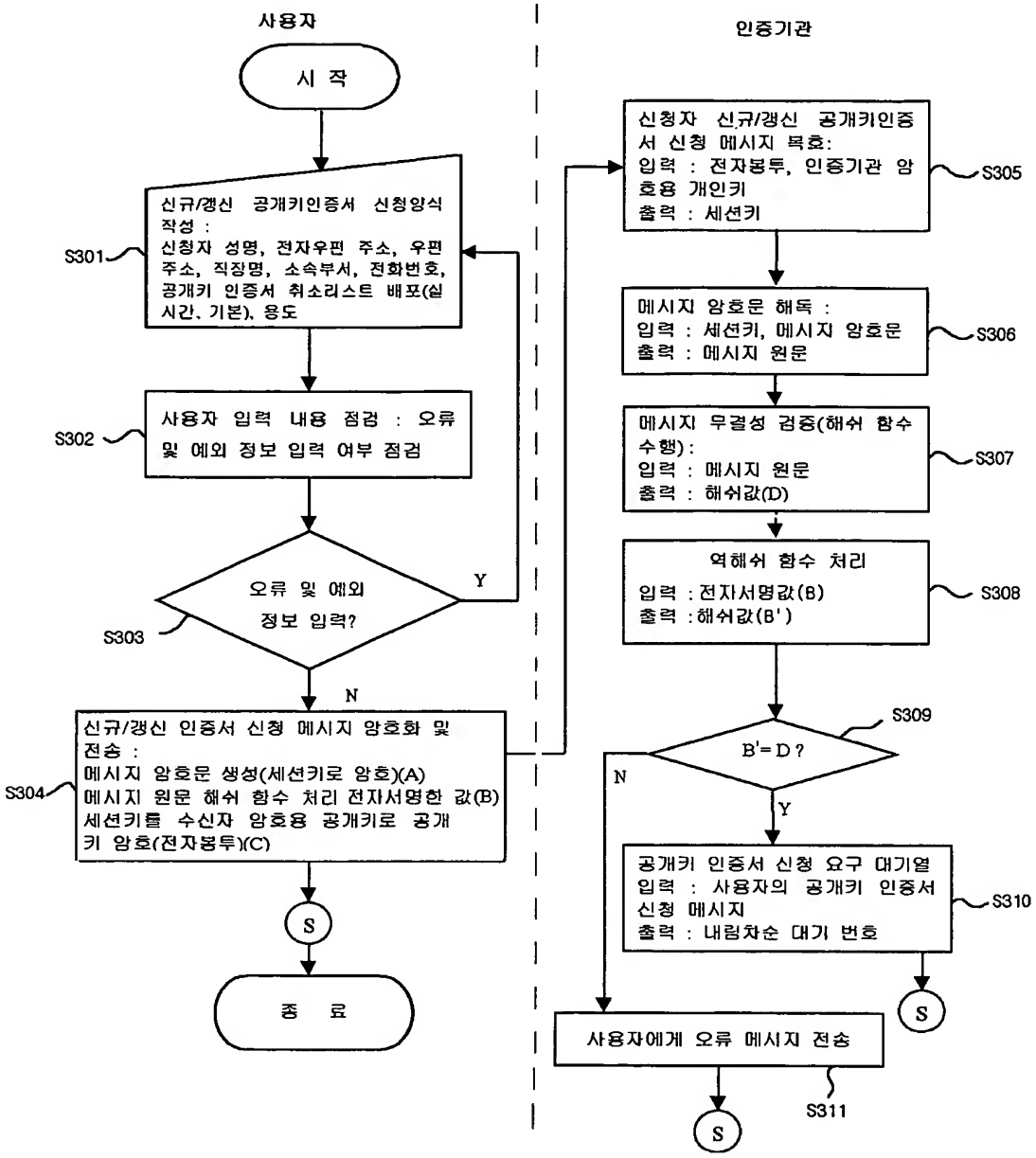
도면 1


사용자의 공개키 인증서 신청 (1)
신청 대기열(2)
(선입선출 방식)
공개키 인증서 생성 작업 로그 관리 모듈(5)
공개키 인증서 생성모듈(3)
공개키 인증서 관리 모듈(4)

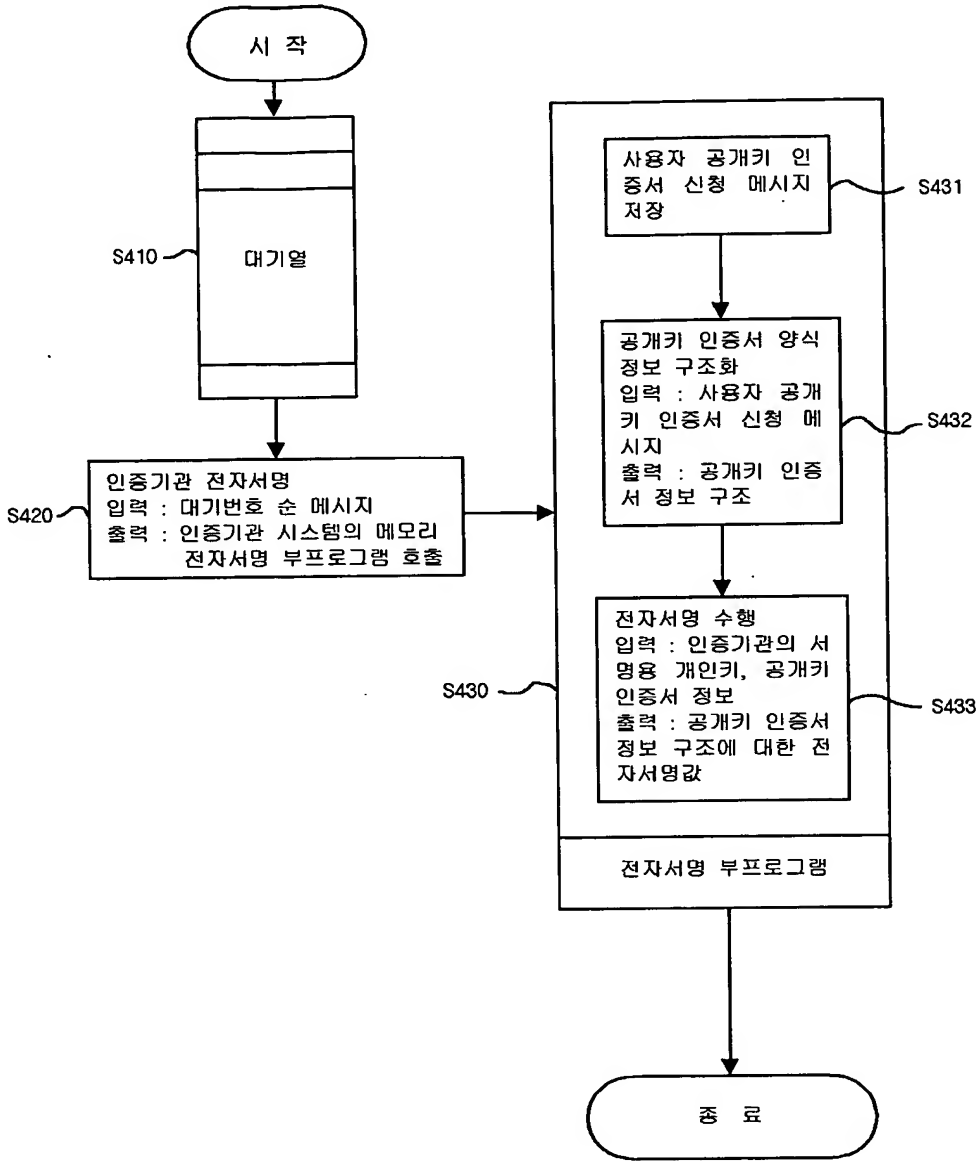
도면 2


시 작
S201
인증기관 관리자의 인증기관 시스템 구동명령 입력: 관리자 암호, 구동 명령어 입력
S202
인증기관 관련 프로그램 구동 -> 프로그램 리스트 참조 후 구동 개시
S203
인증기관의 서명용 및 암호용 키쌍 보유?
Y
S204
기존 키쌍을 임시 저장소에 보관
N
S205
서명용 및 암호용 키쌍 생성 및 상위 인증기관에 공개키 등록(인증기관의 공개키 인증서 발급):
상위 인증기관 방문, 오프라인 방식으로 공개키 인증서 발급 받음
S206
인증기관 시스템 초기화 점검 :
인증기관 서명용 및 암호용 키쌍 보유 유무
인증기관의 공개키 인증서 보유 유무
구동 프로그램 리스트의 프로그램 구동 여부
->관리자 메뉴에서 공개키 인증서 생성 현황 확인
종 료

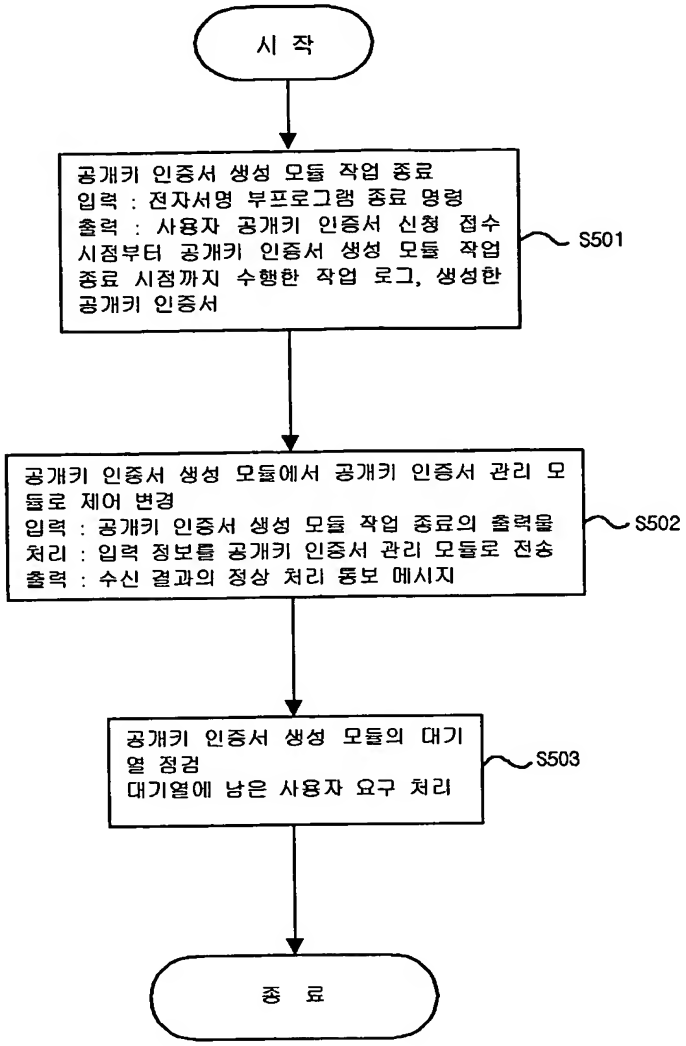
도면 3


사용자
인증기관
시 작
신규/갱신 공개키인증서 신청양식 작성 :
신청자 성명, 전자우편 주소, 우편 주소, 직장명, 소속부서, 전화번호, 공개키 인증서 취소리스트 배포(실시간, 기본), 용도
S301
사용자 입력 내용 점검 : 오류 및 예외 정보 입력 여부 점검
S302
오류 및 예외 정보 입력?
S303
Y
N
신규/갱신 인증서 신청 메시지 암호화 및 전송 :
메시지 암호문 생성(세션키로 암호)(A)
메시지 원문 해쉬 함수 처리 전자서명한 값(B)
세션키를 수신자 암호용 공개키로 공개키 암호(전자봉투)(C)
S304
S
종 료
신청자 신규/갱신 공개키인증서 신청 메시지 복호:
입력 : 전자봉투, 인증기관 암호용 개인키
출력 : 세션키
S305
메시지 암호문 해독 :
입력 : 세션키, 메시지 암호문
출력 : 메시지 원문
S306
메시지 무결성 검증(해쉬 함수 수행):
입력 : 메시지 원문
출력 : 해쉬값(D)
S307
역해쉬 함수 처리
입력 : 전자서명값(B)
출력 : 해쉬값(B')
S308
B'=D?
S309
N
Y
공개키 인증서 신청 요구 대기열
입력 : 사용자의 공개키 인증서 신청 메시지
출력 : 내림차순 대기 번호
S310
S
사용자에게 오류 메시지 전송
S311
S

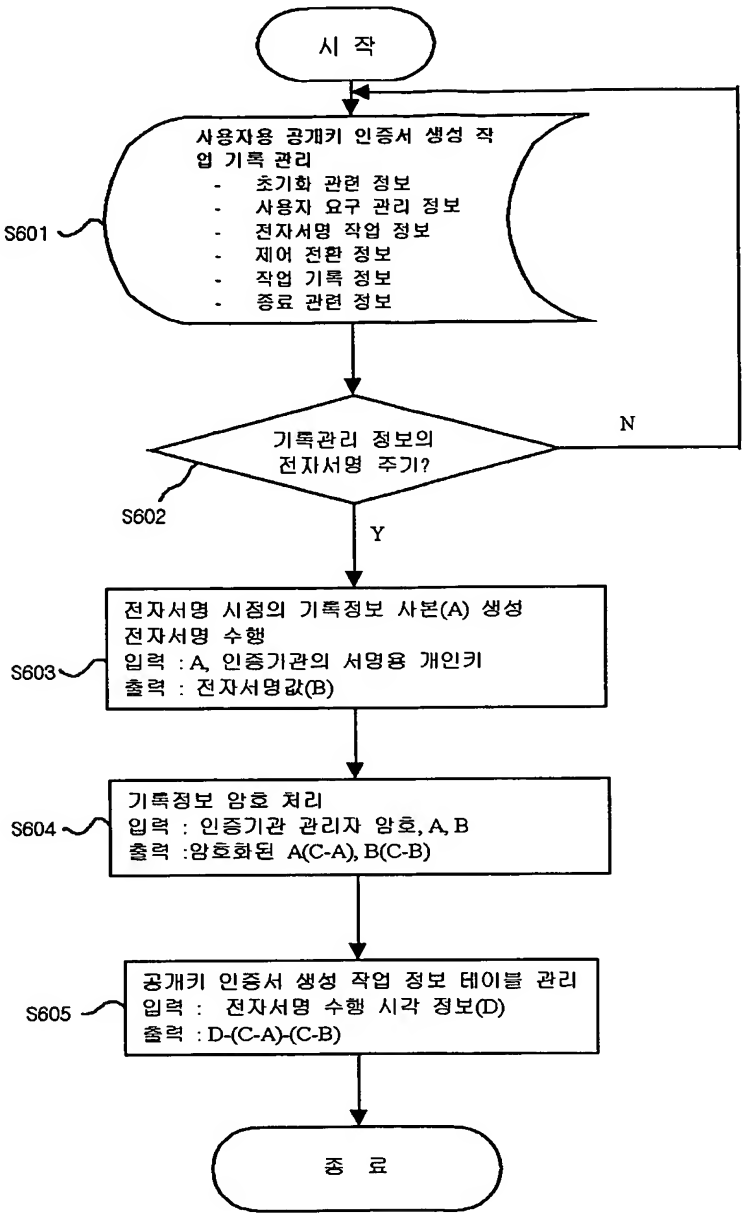
도면 4


시 작
S410
대기열
S420
인증기관 전자서명
입력 : 대기번호 순 메시지
출력 : 인증기관 시스템의 메모리
전자서명 부프로그램 호출
S430
사용자 공개키 인증서 신청 메시지 저장
S431
공개키 인증서 양식 정보 구조화
입력 : 사용자 공개키 인증서 신청 메시지
출력 : 공개키 인증서 정보 구조
S432
전자서명 수행
입력 : 인증기관의 서명용 개인키, 공개키 인증서 정보
출력 : 공개키 인증서 정보 구조에 대한 전자서명값
S433
전자서명 부프로그램
종 료

도면 5


시 작
공개키 인증서 생성 모듈 작업 종료
입력 : 전자서명 부프로그램 종료 명령
출력 : 사용자 공개키 인증서 신청 접수 시점부터 공개키 인증서 생성 모듈 작업 종료 시점까지 수행한 작업 로그, 생성한 공개키 인증서
S501
공개키 인증서 생성 모듈에서 공개키 인증서 관리 모듈로 제어 변경
입력 : 공개키 인증서 생성 모듈 작업 종료의 출력물
처리 : 입력 정보를 공개키 인증서 관리 모듈로 전송
출력 : 수신 결과의 정상 처리 통보 메시지
S502
공개키 인증서 생성 모듈의 대기열 점검
대기열에 남은 사용자 요구 처리
S503
종 료

도면6


시 작
사용자용 공개키 인증서 생성 작업 기록 관리
- 초기화 관련 정보
- 사용자 요구 관리 정보
- 전자서명 작업 정보
- 제어 전환 정보
- 작업 기록 정보
- 종료 관련 정보
S601
기록관리 정보의 전자서명 주기?
N
S602
Y
전자서명 시점의 기록정보 사본(A) 생성
전자서명 수행
입력 : A, 인증기관의 서명용 개인키
출력 : 전자서명값(B)
S603
기록정보 암호 처리
입력 : 인증기관 관리자 암호, A, B
출력 :암호화된 A(C-A), B(C-B)
S604
공개키 인증서 생성 작업 정보 테이블 관리
입력 : 전자서명 수행 시각 정보(D)
출력 : D-(C-A)-(C-B)
S605
종 료